Neapolis University Pafos, Cyprus
AI-2-TRACE-CRIME
Jean Monnet Center of Excellence
Co-funded by the European Union

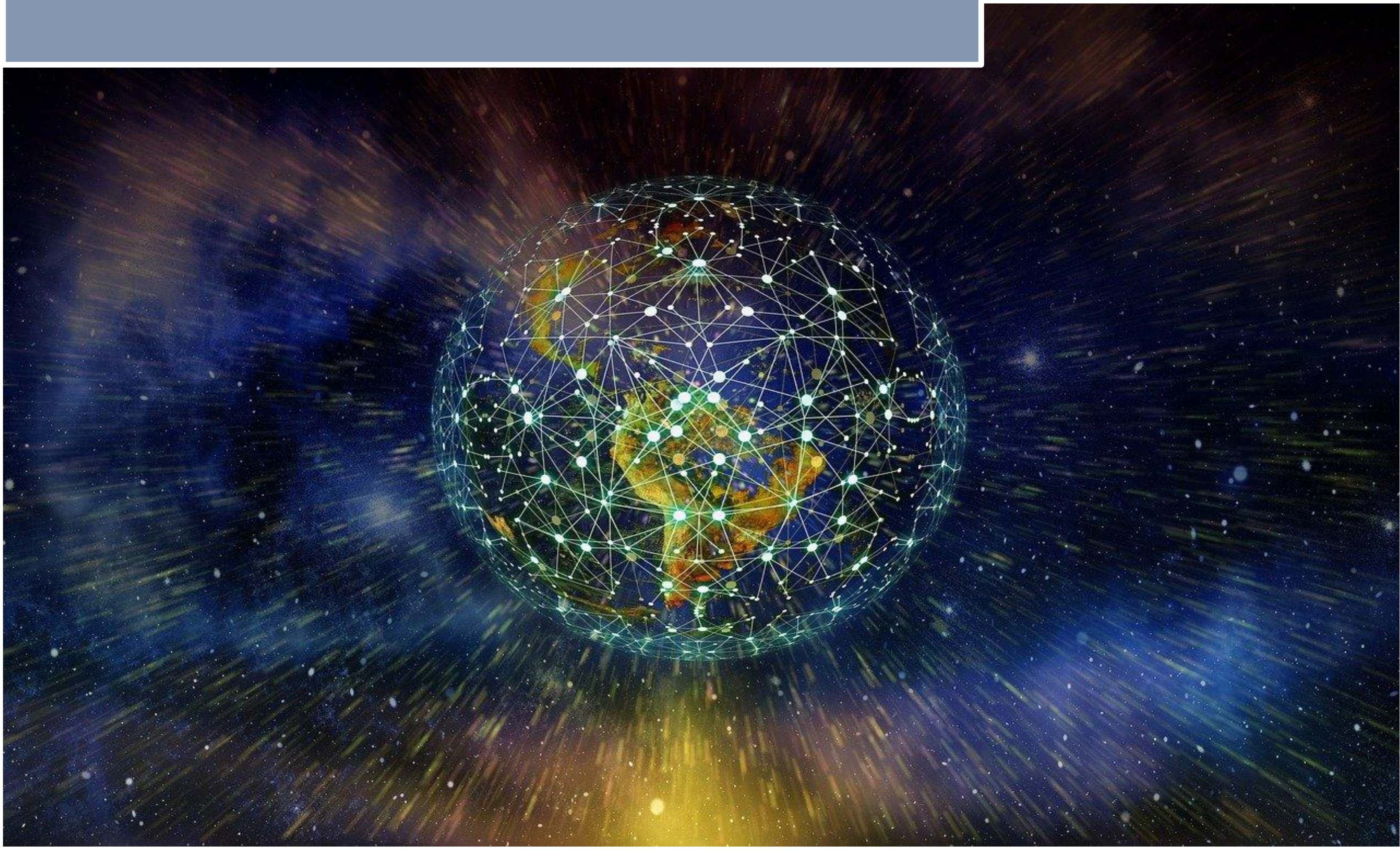
Policy Brief

The Changing Landscape of Cyber-Enabled Crime:

Insights from Europol's IOCTA

NUP Jean Monnet / UNESCO Policy Briefs

41/2026



Co-funded by the European Union

Neapolis University Pafos

UNESCO Chair in Human Development, Security & the Fight against Transnational Crime and Illicit Trafficking in Cultural Property

unesco Chair

The NUP Jean Monnet / UNESCO working papers and policy briefs can be found at:

https://www.nup.ac.cy

Publications in the Series should be cited as:

AUTHOR, TITLE, NUP UNESCO/JEAN MONNET WORKING PAPER or POLICY BRIEF NO. x/YEAR [URL]

Copy Editor: G. Pavlidis

© AI-2-TRACE CRIME

Neapolis University Pafos, School of Law

Pafos, 8042, Cyprus

Frontpage picture: Gerd Altmann from Pixabay

The support of the European Commission and of UNESCO for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors; the European Commission and UNESCO cannot be held responsible for any use which may be made of the information contained therein.

The Changing Landscape of Cyber-Enabled Crime: Insights from Europol's IOCTA

Executive Summary

Europol's Internet Organised Crime Threat Assessment (IOCTA) 2025, titled 'Steal, Deal, Repeat', presents an in-depth examination of the evolving dynamics of cyber-enabled and cyber-dependent crime across the European Union. The report consolidates intelligence from Member States, Europol's operational data, and private sector partners to outline key developments, threats, and emerging patterns within the cybercrime ecosystem.

The 2025 assessment confirms that ransomware continues to pose the most significant cybercrime threat to EU institutions, businesses, and critical infrastructure. Online fraud and scams have become industrialised, operating through large-scale criminal networks that leverage social engineering and data leakage for profit. The proliferation of child sexual exploitation material (CSEM), dark web marketplaces, and crypto-facilitated money laundering underscore the cross-cutting nature of digital criminality.

The IOCTA further highlights that cybercrime is increasingly intertwined with organised crime structures and geopolitical instability. Europol calls for a strengthened, coordinated European approach that combines prevention, law enforcement, public-private collaboration, and technological resilience.

Keywords

Europol, IOCTA, Cybercrime, Ransomware, Online Fraud, Darknet, Child Sexual Exploitation, Virtual Assets, Law Enforcement Cooperation, EMPACT, Cybersecurity.

Background

The Internet Organised Crime Threat Assessment (IOCTA) is Europol's flagship strategic analysis report, produced annually by the European Cybercrime Centre (EC3). It provides a consolidated overview of trends in cybercrime affecting the EU and informs strategic and operational priorities under the European Multidisciplinary Platform Against Criminal Threats (EMPACT).

IOCTA 2025 builds upon nearly a decade of assessments and reflects the growing convergence between traditional organised crime and cybercrime. Its findings support EU policy development in areas such as digital resilience, data protection, and criminal justice cooperation. The report also feeds into the implementation of the EU Cybersecurity Strategy and the Digital Services Act (DSA) framework, reinforcing the need for coherent responses across sectors.

Key Trends Identified in IOCTA 2025

The IOCTA 2025 identifies several dominant trends shaping the European cybercrime landscape:

- Ransomware Dominance: Ransomware remains the most disruptive cyber threat. Attackers increasingly use double and triple extortion models, combining data theft, encryption, and threats of exposure to pressure victims.

- Industrialisation of Online Fraud: Fraud schemes have evolved into a professionalised economy. Criminals operate call centres, phishing-as-a-service models, and investment scam platforms that target individuals and corporations alike.

- Darknet Market Adaptation: Despite law enforcement takedowns, darknet marketplaces continue to re-emerge, offering illicit goods, data, and hacking tools. Cryptocurrency mixing services remain central to conceal criminal proceeds.

- Child Sexual Exploitation Material (CSEM): The production and distribution of CSEM have increased, driven by online platforms, encrypted communications, and cloud storage abuse.

- Convergence with Organised Crime: Traditional criminal groups increasingly use digital tools for logistics, recruitment, and financial operations, blurring boundaries between cyber and conventional crime.

The report stresses that these developments are mutually reinforcing, creating a self-sustaining criminal ecosystem characterised by innovation and adaptability.

Operational and Policy Implications

The findings of IOCTA 2025 have direct implications for both operational enforcement and policy design within the EU. Cybercrime has become a horizontal threat cutting across domains, requiring an integrated and multi-agency response.

Key implications include:

- The need for harmonised digital evidence frameworks to facilitate cross-border investigations;

- Continued prioritisation of ransomware, online fraud, and child sexual exploitation under EMPACT 2026–2030;

- Enhanced capacity for tracing virtual assets and dismantling cryptocurrency laundering networks;

- Development of specialised cybercrime units and public-private task forces to address the industrialisation of online fraud;

- Promotion of cyber hygiene, awareness campaigns, and victim reporting mechanisms to strengthen resilience.

Europol emphasises that operational success depends on sustained cooperation between national law enforcement, judicial authorities, and private sector actors.

EU and International Cooperation

Europol's coordination role remains central to the EU's collective response to cybercrime. Through the European Cybercrime Centre (EC3) and its Joint Cybercrime Action Taskforce (J-CAT), Member States collaborate on joint investigations, information exchange, and intelligence analysis.

The IOCTA 2025 report underlines the importance of cooperation with EU institutions such as the European Union Agency for Cybersecurity (ENISA), Eurojust, and the European Public Prosecutor's Office (EPPO), as well as partnerships with Interpol and non-EU states. These efforts are complemented by Europol's initiatives in digital forensics, malware analysis, and operational threat monitoring.

Internationally, Europol supports cross-border collaboration through liaison networks, coordinated takedowns, and capacity-building projects aimed at improving digital investigative capabilities.

Challenges and Strategic Priorities

The IOCTA identifies several strategic challenges that hinder an effective EU-wide response to cybercrime:

- Fragmented legal frameworks for digital evidence collection and data retention;

- Shortage of skilled cyber investigators and forensic experts;

- Limited public awareness and underreporting of cyber incidents;

- Dependence on third-country digital infrastructure, complicating jurisdictional enforcement;

- Need for consistent metrics to evaluate operational outcomes and threat trends.

To address these challenges, Europol recommends a multi-layered strategy centred on deterrence, detection, and disruption. Priorities include improved analytical interoperability, enhanced cyber resilience of critical infrastructure, and sustained investment in technology and training.

Concluding Remarks

The 2025 IOCTA reaffirms that cybercrime has evolved into a systemic threat to Europe's digital security, economy, and trust in technology. Europol's analysis underscores that combating this threat requires coordinated action at both the national and EU levels, integrating prevention, enforcement, and innovation. The growing overlap between cybercrime, organised crime, and financial fraud calls for continuous adaptation of legal frameworks and operational tools.

A resilient Europe depends on collective vigilance, technical capacity, and public-private solidarity. The IOCTA serves as both a warning and a roadmap—highlighting the urgency of proactive measures to secure Europe's digital future.

Further Reading

- Europol (2025), Internet Organised Crime Threat Assessment (IOCTA) 2025 – 'Steal, Deal, Repeat' (link)